CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:

a processor;

a device coupled to the processor, wherein the device includes:

one or more sub-devices; and

one or more access locks, wherein the one or more access locks are configured to prevent access to the one or more sub-devices when the one or more access locks are engaged.

2. The system of claim 1, wherein the device includes a bridge.

3. The system of claim 1, wherein the one or more sub-devices include one or more from the group consisting of:

a duration timer;

mailbox RAM;

locks for a storage device;

overrides for the locks for the storage device;

a TCO counter;

a monotonic counter;

scratchpad RAM; and

a random number generator.

4. The system of claim 1, wherein the one or more access locks include a single access lock configured to prevent access to a plurality of the one or more sub-devices when the single access lock is engaged.

5. The system of claim 4, wherein the single access lock includes a sequester register configured to store a sequester bit.

6. The system of claim 1, wherein the one or more access locks include two or more access locks, wherein a first access lock is configured to prevent a first access to a plurality of the one or more sub-devices when the first access lock is engaged, and wherein a second access lock is configured to prevent a second access to a plurality of the one or more sub-devices when the second access lock is engaged.

7. The system of claim 6, wherein the first access is a read operation, and wherein the second access is a write operation.

8. The system of claim 1, wherein the one or more access locks include a plurality of sequester registers.

9. The system of claim 8, wherein each of the plurality of sequester registers is configured to prevent access to a different one of the one or more sub-devices when engaged.

10. The system of claim 9, wherein each of the plurality of sequester registers is configured to store one bit.

11. The system of claim 9, wherein each of the plurality of sequester registers is configured to store a plurality of bits.

12. A method of operating a computer system in SMM, the computer system including a processor coupled to a memory, to security hardware, and to a first device, the method comprising:

unlocking security hardware;

accessing a first device;

locking the security hardware; and

calling an SMM exit routine.

13. The method of claim 12, further comprising:

checking a lock status of the security hardware.

14. The method of claim 12, further comprising:

processing SMM code instructions.

15. A computer system configured to operate in SMM, the computer system comprising:

means for unlocking security hardware;

means for accessing a first device;

means for locking the security hardware; and

means for calling an SMM exit routine.

16. A computer readable program storage device encoded with instructions that, when executed by a computer system including a processor coupled to a memory, to security hardware, and to a first device, performs a method of operating a computer system in SMM, the computer system, the method comprising:

unlocking security hardware;

accessing a first device;

locking the security hardware; and

calling an SMM exit routine.

17. The computer readable program storage device of claim 16, the method further comprising:

checking a lock status of the security hardware.

18. The computer readable program storage device of claim 12, the method further comprising:

processing SMM code instructions.